

**AN ASSESSMENT OF THE IMPACT OF THE EXPORT OF
ADVANCED COMPUTERS AND COMPUTATION TECHNOLOGY
ON THE PROLIFERATION OF CONVENTIONAL WEAPONS,
WEAPONS OF MASS DESTRUCTION, AND THEIR MEANS OF
DELIVERY**

PREPARED FOR
THE COMMITTEE ON NATIONAL SECURITY
U.S. HOUSE OF REPRESENTATIVES

Stephen Bryen
William R. Graham
Phil Marcus
William Schneider, Jr.

July 15, 1977

AN ASSESSMENT OF THE IMPACT OF THE EXPORT OF ADVANCED COMPUTERS AND COMPUTATION TECHNOLOGY ON THE PROLIFERATION OF CONVENTIONAL WEAPONS, WEAPONS OF MASS DESTRUCTION, AND THEIR MEANS OF DELIVERY

1.0 Introduction

This report responds to a request (April 16, 1997) of the Chairman of the Committee on National Security (Hon. Floyd Spence, MC) and the Ranking Member (Hon. Ron Dellums) of the US House of Representatives to undertake a review of the impact of an October, 1995 US government decision to liberalize export controls on U.S. supercomputers. The Committee's request is derived from the report of the Committee of Conference accompanying the National Defense Authorization Act for Fiscal Year 1996 (Public Law 104-106). In the report, the Congress expressed concern over "the potential impact of this decision [the October, 1995 US government decision to liberalize supercomputer exports] on the United States' nonproliferation efforts and the maintenance of the US military technological edge" and directed the Secretary of Defense to submit a report describing "the impact of the export decision on the ability of nations to acquire and use high-performance computing capabilities to develop advanced conventional weaponry, weapons of mass destruction (WMD), and delivery vehicles including missiles." In response to this requirement, a study conducted (S. Goodman et al, Building on the Basics: An Examination of High Performance Computing Export Control Policy in the 1990s, Stanford University, August, 1995) by the Center for International Security and Arms Control of Stanford University was submitted to the Committee by the Department of Defense. A copy of the report for the public record was submitted to the Committee by the Under Secretary of Commerce for Export Administration in April, 1997.

This report responds to the Committee's request to review and comment on the following issues raised by the DoD-sponsored study:

1. Review the study's assumptions, methodologies, and conclusions.
2. Examine whether the October, 1995 decontrol decision and subsequent modification of export regulations have made it easier for unapproved transfers of US high performance computing capabilities to take place and, if so, to offer suggestions to more appropriately constrain such transfers.
3. Provide observations on how the computing capabilities of the Silicon Graphics and similar machines [provided to the Russian Chelyabinsk-70 nuclear weapons facility] could be exploited by potential adversaries, including Russia.

4. Assess the overall implications of the transfer to nations abroad of high performance computing on US national security.

2.0 National security aspects of the regulation of high performance computers and computer technologies.

2.1 Cold-War export control aims, practices, and consequences.

The regulation of high performance computation has been a central feature of post World War II export control practices as the concept of national security controls was broadened from defense products and services to enabling scientific and industrial equipment, technologies, and services associated with defense equipment. During the 1950s and '60s, the dominance of the United States in high performance computation technology, the high cost of these systems, and their limited production made the regulatory process a relatively simple one. The US defense establishment was a key factor in imposing demanding performance requirements for computation to meet national security requirements. These requirements included nuclear weapon design, development, manufacture, and test, networked air defense, anti-submarine warfare, and intelligence collection and processing. The civil sector demand for advanced computation grew rapidly in the 1970s and '80s, overtaking the defense sector as the driving force in the demand for high performance computing.

The rapid growth in the demand for high performance computing in the 1970s and '80 reflected the impact of a succession of generational changes in computing technology that produced exponential increases in performance accompanied by parallel reductions in cost, weight, and volume. These new computing technologies were accompanied by improvements in software engineering which in turn created new scientific and industrial as well as national security applications for high performance computing.

The linkage between computers and both direct military applications and indirect applications to Soviet military power through its defense-industrial base came to be understood during the 1980s. Intelligence data revealed the role access to Western computation technology played in intelligence collection priorities of the two leading Soviet intelligence services during the 1970s (the Soviet government's KGB and the armed forces' GRU). The impact of access to Western computing (and other advanced technologies) acquired by the Soviet intelligence services in the 1970s on the modernization of Soviet strategic and general purpose forces equipment began to appear in Soviet military deployments in the early 1980s.

The emergence of the intensified threat to the Western alliance led to a considerable strengthening of the process of multilateral export controls, particularly the Coordinating Committee on Multilateral Export Controls (COCOM). COCOM was able to adapt to the impact of the diffusion of computer-related technology. The list of controlled

technologies was subject to more frequent review permitting liberalization of “commodity” computers as technology evolved. Diplomatic processes extended the “reach” of COCOM controls to non-member states to contain Soviet-bloc efforts to acquire advanced computing hardware, services, and technologies from or through non-member states. Comprehensive and responsive support from the US intelligence community facilitated effective enforcement of COCOM restrictions in the US, and made it possible for US diplomats to strengthen the effectiveness of allied nation enforcement as well. The COCOM objective of “equal enforcement” among members was an important objective for both the effectiveness of the export control regime, and to preserve a “level playing field” for industrial producers throughout the alliance.

The imposition of effective multilateral export controls on high performance computing during the latter stage of the Cold War proved fortuitous. The implications of digital technology for military applications had come to be appreciated by the Department of Defense creating what has become known as the “Revolution in Military Affairs.” While the former Strategic Defense Initiative (SDI) became a metaphor for the military applications of high performance computing, it was by no means the most significant example of the coupling between high performance computing and advanced military capabilities. Although the operation of a large-scale missile defense would inevitably involve high performance computation, the SDI was not the pacing element in high performance computing developments during the 1980s. The scientific and industrial role of high performance computing for the real and near-real time modeling of physical phenomena was notably more important as a contributor to the RMA and is likely to be an enduring dimension of the application high performance computing.

Effective export controls were an important dimension of the USG “policy mix” used to confront Soviet military power in the 1980s. Export controls served to deny the former Soviet Union (FSU) access to militarily useful advanced technology including high performance computing. At the same time, the increased demands for such technologies to compete with American advances in the RMA (including SDI) contributed to ending the Cold War, according to a recent historical study of the period. Former Soviet President Mikhail Gorbachev’s remark at the 1985 Reykjavik Summit meeting to former President Reagan to the effect that the FSU was unable to compete with the US in military capabilities as a consequence of its inability to gain access to advanced technologies underscores the coupling of advanced technology to military performance and its impact on the diplomacy of the Cold War.

The special role of advanced computation was recognized in the early 1980s. Prior to that time, the United States was the sole producer of machines that were defined (by the rate of performance of operations per unit time) as supercomputers. As the US government imposed a presumption of denial on such exports, a multilateral regime was unnecessary. However, supercomputers involving both vector and parallel processing in

other nations began to emerge during the early 1980s, particularly in Japan. This led to bilateral efforts to control the dispersion of supercomputer technology, most significantly in the US-Japan supercomputer agreement in 1984. This arrangement was eventually institutionalized and control benchmarks established. The administration sought an order of magnitude lifting of the ceiling from 195 Mtops (Millions of theoretical operations per second) to 2,000 Mtops. Japan was only prepared to agree to raising the ceiling to 1,500 Mtops. The administration unilaterally decontrolled computers capable of operations up to the old supercomputer benchmark – 2,000 Mtops.

2.2 Post Cold War export control policies, practices, and national security consequences concerning high performance computing.

The collapse of the FSU in 1991 was led by the end of Communist rule in Central Europe following the opening of the Berlin Wall in 1989. The institutional basis for multilateral export controls for advanced technology, dual use items, and munitions list products and services was concentrated in the COCOM apparatus. Other multilateral “supplier clubs” were established to support the aims of multilateral non-proliferation regimes with virtually universal membership. The London Suppliers group of key Western industrial exporters of nuclear technology augmented the enforcement arrangements associated with the Nuclear Non-Proliferation Treaty (NPT) of 1968 to address the limited capabilities of the United Nation’s International Atomic Energy Agency (IAEA). Despite the specific aims of the agreement, and the near-universality of its membership, it has not been able to prevent evasion of its terms by proliferation-inclined members (e.g. Iraq, North Korea, etc.)

The Missile Technology Control Regime of 1987 provided a non-treaty based export control regime for military missiles and major subsystem technology. Informal cooperation among signatories provides a basis for diplomatic collaboration to discourage the transfer of controlled items. However, the scope of the MTCR does not engage enabling scientific and industrial technologies associated with the development, production, and testing of military missiles. As a consequence, more nations are developing, manufacturing, or using military missiles embodying MTCR-controlled technologies since the end of the Cold War than was the case during the period.

The Australia Group was established to facilitate the control of exports of chemical agents and precursor chemicals to sensitive destinations. The aims of the Australia Group have been reinforced as “international norms” by ratification of the Chemical Weapons Convention (CWC) by the US Senate in April, 1997. The effectiveness of the CWC and the supporting Australia Group controls will depend on the universality of membership and adherence to the provisions of the CWC.

The end of the military threat posed by the FSU and its Warsaw Pact military alliance stimulated a substantial liberalization in US dual use export controls. The scope of the

liberalization is reflected in the aggregate statistics of the issuance of validated export licenses. In the mid-1980s, nearly 150,000 validated dual-use export licenses were issued per year by the Department of Commerce. Despite a significant increase in the volume of advanced technology trade in the ensuing decade, successive waves of liberalization reduced the scope of export controls so substantially that less than 10,000 licenses are issued annually today.

Multilateral export controls on militarily significant dual-use technology largely ended in 1993 when COCOM was disestablished. After three years of difficult negotiations, COCOM was replaced by an organization with broader membership (e.g. including Russia), but with a far narrower scope. The new organization -- the Wassenaar Arrangement -- began work in 1996. The Wassenaar Arrangement focuses on restricting the export of munitions list equipment and services to "sensitive" destinations such as Iran, Iraq, and Libya. However, the organization does not address transfers of enabling dual-use scientific and industrial technology needed to develop military systems and subsystems, nor does it provide for pre-notification of sales of munitions list equipment to sensitive destinations. Improving the effectiveness of the Wassenaar Arrangement is an important non-proliferation priority of the US government.

Restrictions on the export of munitions list technology by most major allied nations in addition to the United States for several end users including China, Iran, and Iraq has produced a significant change in the approach of these nations to conventional weapons modernization, WMD, and missile development, manufacturing, and testing. Although some military equipment continues to flow to these nations from some foreign producers, these nations have increasingly emphasized the acquisition of advanced development and manufacturing technologies through international commerce. The liberalization of access to such technologies has been extensive since 1989, and in the case of supercomputers, has been accelerated since 1993. The advanced technology defense manufacturing sectors (including high performance computers) in China, Iraq, and Iran are primarily supplied by the United States and allied nations.

2.3 Trends in defense technology pertinent to export control decisions on high performance computers and associated technologies.

High performance computing technology is a typical, though important example of a significant underlying trend affecting the defense-industrial aspects of national security policy. The demands for higher performance computing and most other areas of technology pertinent to national defense are driven by civil and commercial requirements, not national defense. Indeed, in many areas, the application of advanced technology including high performance computers is more intense in the civil and commercial sector than is the case in the defense sector. To a considerable degree, these circumstances reflect the institutional aspects of defense procurement whose imperatives (e.g. DoD's isolated and unique procurement process) slow the transfer of advanced technology in

the United States from the civil sector to defense applications. The defense procurement process has made it difficult to transfer advanced technology from the civil sector to defense application in a timely manner. The manner in which military specifications produce a protracted process of development, manufacturing, and testing is inconsistent with many areas of advanced technology, including high performance computing, where technical obsolescence overtakes the ability of the defense procurement system to accommodate such change.

Former Secretary of Defense William Perry recognized the dangers to American security inherent in the difficulties the DoD procurement process created for the timely transfer of advanced civil sector technology to national security applications. A set of measures known as the "Perry Initiatives" have sought to break down the regulatory barriers to the more rapid exploitation of advanced civil sector technology. The "Perry Initiatives" are widely regarded as an effort to facilitate the evolution of the US defense posture from one dependent on "industrial" technology to one which exploits the capabilities of "information" technology.

The conclusions of the Quadrennial Defense Review (QDR) published on May 15, 1997 suggest the trend toward the use of advanced technology developed for civil and commercial applications by the DoD and defense-industrial suppliers for military purposes will intensify in the first two decades of the 21st century. Although the institutional arrangements in nations abroad, especially in proliferation prone nations, is likely to differ substantially from American practice in the manner in which they apply such technology for military purposes, it appears inevitable that high performance computing will be an important dimension of the military modernization process in all countries, both allied and adversarial.

3.0 An assessment of the assumptions, methodologies, and conclusions of "Building on the Basics: An Examination of High-performance Computing Export Control Policy in the 1990s."

This assessment is based upon the text of the study supplied to the Committee on National Security of the US House of Representatives.

3.1 Assumptions

The study is based upon the analysis of the application of high-performance computing to four broad areas of military activity:

- nuclear weapons programs
- cryptology

- conventional weapons programs
- military operations

This assumption that high performance computing requirements in these areas of military activity reflect the most significant aspects of concern has caused the authors to concentrate on the analysis of the application of high performance computing to these activities. This assumption is, however, too narrow to be useful for purposes of the analysis of export control policy. These applications are the “tip of the iceberg” of high performance computing applications for national defense. All but the conventional weapons program category are tightly controlled military applications or are performed in a contractor environment that is largely dedicated to defense purposes. For these specialized applications, defense requirements are crucial for driving high performance computing requirements.

However, as defense-related research and production account for a declining share of the advanced technology economy in the United States, the DoD will be dependent on the civil sector to supply advanced technology products whose characteristics are substantially dependent on high performance computing capacity. Decisions on computer usage in these circumstances is not dependent on either the Department of Defense or the Federal Acquisition Regulations (FARs) or other institutional arrangements controlled by the Federal government. The scope of technology available for national defense purposes will be determined by the civil sector, not the Department of Defense.

By concentrating the analysis of DoD requirements on a set of specific military applications, the study understates the role of high performance computing in defense research and modernization. Conclusions drawn from this assumption are likely to misstate the significance of high performance computing for military applications by nations abroad.

A second assumption which constrains the value of the study to the Congress as a basis for the evaluation of export controls is the exclusive focus on American defense applications of high performance computing. The process of deriving conclusions for export policy based upon an analysis of US practice – “mirror imaging” – was a frequently practiced vice of Cold War-era analysis that often led to inappropriate conclusions.

The purpose of export controls in the non-proliferation context is to restrict the ability of proliferation prone states from acquiring advanced technology – including high performance computers – that can abet their military modernization aspirations. Export controls need to be designed to reflect the manner in which proliferators seek to achieve

their aims. The pattern of proliferation in nations such as China, Iran, and Iraq does not closely parallel the manner in which the US defense establishment uses high performance computing for defense purposes. Evidence collected by the UN Special Commission on Iraq (UNSCOM) underscores the need to design non-proliferation export control regimes in a manner which will have a significant impact on the degree of success enjoyed by potential proliferators. By mirror-imaging US practice on proliferators abroad in the proposed design of export controls, China, Iran, Iraq, and other proliferators are likely to be little affected by US non-proliferation measures.

3.2 Methodology

The study identifies a number of major developments in advanced military applications such as stealth, theater missile defense, advanced tactical aircraft development, optical tracking and target recognition, anti-submarine warfare, and others. Computing capabilities used by the USG or industry to develop, operate or produce existing systems are identified. In a number of cases, minimum computing requirements that could have been used to develop, operate, or produce the system or service are described. In most cases, the minimum computer requirements needed to provide the desired design or production capability are less, often significantly less than available from the computer(s) used to support the development, operating, or manufacturing activity.

While this methodology is useful from the perspective of chronicling the historic computer hardware requirements for the development of major US military systems and service support, its utility for the purpose intended -- assessing high performance computing export control policy -- is more limited. The US defense-industrial establishment is rich in high performance computing systems resources. These widely distributed capabilities in hardware are supported by a development and vendor base providing enabling technologies and services ranging from special purpose software to advanced displays to distributed architectures of networked systems of high performance computers. The performance capabilities embedded in the scientific and industrial processes which produced systems such as the F-22 are not only a product of advanced computation for the signature management of the platform itself, the functioning of weapon systems is computationally intense. The extensive use of high performance computing in the United States and its key allies to develop, operate, and manufacture sophisticated and cost-effective military equipment and "systems of systems" reflects the breadth and depth of the utilization.

Thus, the pertinence of high performance computing resources for advanced military applications is only partially reflected in its application to "cutting edge" defense capabilities. From an export control perspective, the issue of concern is the potential impact of the transfer of high performance computing capabilities and associated support hardware and software services on the ability of the recipient (adversary) nation to produce effective countermeasures and countervailing or asymmetric military

capabilities. The effectiveness of high performance computing to accelerate the development of countervailing military capabilities, increase their performance, and reduce their cost can have an adverse effect on US security and foreign policy objectives. As a result, the assessment of export controls on high performance computing cannot be resolved by extrapolation from the context in which high performance computing is used in the United States defense industrial apparatus. The issue of the role of export controls in managing the diffusion of high performance computing capabilities is, in turn, separable from the issue of the ability of the export control enforcement apparatus to achieve effective access limitations on the controlled high performance computing technology.

3.3 Conclusions

The study produces a number of conclusions pertinent for the assessment of the relevance of export controls on high performance computing. These conclusions will be analyzed separately with respect to the issue of export control policy.

1. *There exist a significant number of applications of national security concern with extensive computational support requirements. Proliferation of some of these applications could be slowed or prevented through export controls on high performance computing [HPC].*

Comment

The study minimizes the significance of export controls on computers which it asserts are “below the level of controllability”. The study acknowledges that such systems can be used for the computational requirements of first generation nuclear weapon design and many cryptologic applications, but finds the impact on foreign military RDT&E to be “minimal.”. The “model” of computer applications for military purposes taken by the study’s authors reflects an unstated assumption of parallelism in the approach taken by potential adversaries with the manner in which high performance computing is used in the United States. This assumption leads the study’s authors to subsequent conclusions that only controls on leading-edge high performance computing likely to be used in the most advanced military applications (e.g. advanced signal processing, TMD, numerical weather prediction, and optical tracking) with processing capabilities in excess of 7,400 Mtops is pertinent to US security interests. However, computers with performance levels decontrolled by the 1995 decision can contribute to important adversary military capabilities. Denying or limiting access to such systems by sensitive end users would serve US security interests.

2. *There continue to be applications for which clusters or networks of computers cannot be used, and there are groups of HPC requirements above the level of uncontrollability.*

Comment

The study acknowledges that there are national security applications for which neither parallel processing is, nor distributed computer architectures are adequate solutions for military requirements at this time. This is especially true in the case of real/near-real time processing requirements arising from systems deployed in differing environments (airborne, sea, space, and ground based). This conclusion, while correct in our view, understates the functionality of computer systems below current control thresholds for foreign national security applications. Further, the conclusion contains an unstated assumption that access to such computer capabilities for the execution of such applications cannot be affected by export controls because they “are readily available on the international market in the form of expandable computers below the HPC control threshold, or because they can be effectively executed on distributed architectures”.

Such a conclusion does not address computational functionality for military applications; it is an assertion about the ability to manage and enforce export controls for which no evidence is offered. Moreover, it does not address the structure of the employment of advanced technology by proliferators as they seek cope with export controls. A substantial, though incomplete body of evidence is available on the approach taken by the former Soviet Union and the Warsaw Pact to evade rigorous dual-use and munitions list controls employed during the Cold War period. The success of these export controls attests to the systemic impact of pervasive national security-based controls on the ability of an adversary state or military coalition to challenge US and allied technological advances. When export controls were liberalized, especially on dual use technology during the late 1980s and early 1990s, Pakistan, Iraq and Iran’s evasion of nuclear and missile non-proliferation controls, and China’s efforts to escape the impact of US munitions list export controls in the 1990s were highly successful.

The adaptive behavior forced on the Soviet bloc brought about by effective (multilateral) COCOM export controls and the associated fabric of diplomatic, law enforcement, and intelligence collaboration achieved the intended national security impact on adversaries. The development of the scientific and industrial capacity by the Soviet bloc to pose a national security threat to US interests was disrupted compared to what would have been the case without export controls. As a result, the defense industrial establishment of adversary states suffered the consequences of uneven and covert efforts to acquire controlled technology. The export control system produced program delays, high costs, and ineffective deployed systems in the Soviet bloc, and was reflected in the low rate of utilization of high performance computing in the Soviet defense industrial establishment.

3. *The computing power needed to carry out a very large fraction of applications of national security interest is no longer controllable.*

Comment

The authors of the study acknowledge that a large number – a “very large fraction” – the term used in the study, of high performance computing capabilities are applicable to national security purposes. By derivation, we conclude that such capabilities in the hands of an adversary state may be orthogonal to US national security interests. Factors previously alluded to in the study – international availability and the ability to use distributed architectures to network uncontrolled computers – are asserted as the basis for concluding that the diffusion of advanced computer capabilities of up to 1,000 Mtops cannot be effectively controlled. Illustrative of basic applications of national security interest below the current control threshold are “in the nuclear and cryptography categories”. This conclusion does not deny the potentially adverse coupling of uncontrolled exports of computers and computer technology below current export thresholds. Rather it concludes that international availability and distributed architectures preclude effective controls. The specific issue of export control enforcement will be addressed elsewhere in this report.

4.0 Implications of the US Government’s October, 1995 decision to liberalize high performance computer exports.

The decision by the USG to liberalize high performance computing exports in 1995 accelerated a trend which began in the late 1980s to remove most export controls from dual-use technologies, including high performance computers. The scope of the liberalization is reflected in aggregate statistics of the issuance of validated export licenses by the Department of Commerce. In the mid-1980s, nearly 150 thousand validated export licenses were issued annually. The comprehensive scope of the liberalization of dual-use exports is reflected in the fact that less than 8,000 are issued today, despite a much larger volume of international commerce in advanced technology products, including high performance computing. The intense focus on dual-use export liberalization can be seen in comparative statistics with munitions licensing by the Department of State. Despite a fifty percent decline in exports of defense products and services, the number of munitions licenses issued annually has declined only about twenty percent (approximately 46,000 munitions licenses were issued in FY 96) responding to more extensive regulation of such exports. Not surprisingly, liberalization of dual-use exports has stimulated a refocusing of effort on the part of proliferators in favor of indigenous defense-industrial development. During the Cold War when export controls were pervasive, the preferred route to defense modernization prior to the 1980s was offshore procurement of defense articles and services.

Iraq and Libya in the 1980s, and China and Iran in the 1990s have built up their defense industrial establishment including weapons of mass destruction and their means of

delivery as well as advanced conventional weapons based on access to sophisticated dual use technology from the United States (in the case of China) and the advanced economies of allied nations (in the case of China and Iran). The decontrol of a substantial fraction of high performance computers relevant to significant military capabilities have allowed these computational capabilities to be widely disseminated. The absence of licensing requirements has diminished the ability of the USG to monitor and assess the significance of such developments for US national security purposes until military systems developed with the support of advanced computational capabilities are tested or deployed. The inadvertent consequence of this liberalization initiative has been to facilitate the proliferation of weapons of mass destruction and their means of delivery as well as the development of advanced conventional weapons. The probable surge in the proliferation of advanced conventional and unconventional weapon systems in the early years of the 21st century may require an increase in countervailing US and allied military capabilities in the future.

5.0 Assessment of the significance of Silicon Graphics supercomputer export(s) to the Russian nuclear weapons design/production complex.

Russia's procurement of high performance computers from Silicon Graphics places the policymaker's dilemma in bold relief. USG officials must address the conflicting goals of export promotion and non- and counterproliferation. Despite persuasive tales of privation in Russia's scientific establishment, funds were found by the Russian nuclear weapons establishment to procure the Silicon Graphics supercomputers. The international decision to end nuclear weapon testing appears to have caused Russia's nuclear weapons establishment to look to the means to sustain their nuclear posture (Russia has refused to ratify START II). Russia has initiated programs to develop a new series of sea and land based strategic missiles. It is possible that new nuclear warheads will be required for these missiles that will employ previously tested weapon components (e.g. primary and secondary sections). Russian nuclear weapon designers may need high performance computers to assess the performance, reliability, and safety of these design variations in the absence of testing. Supercomputers provide the means to simulate the physical phenomena associated with some of the properties of the aging of the components of nuclear weapons.

In this respect, the Russian effort may have some parallels to the Clinton administration's Science Based Stockpile Stewardship Program. This program emphasizes an advanced computation initiative along with several other measures to carefully monitor the condition of the residual nuclear weapons inventory in the absence of an opportunity to conduct episodic testing to assure weapon reliability and safety. Due to the absence of export controls on high performance computers below the 1995 threshold, it was not possible for the USG to make a public policy determination on whether or not USG interests were served by providing the means for Russia to maintain the reliability and

performance of its nuclear weapons inventory. This opportunity for a policy determination on this matter was precluded by an earlier decision to liberalize the export of high performance computers.

The liberalization of export controls on high performance computing is likely to provide Russia with the means to advance other computation-intensive military applications. For example, the defense trade press recently reported on a joint Russian and Israeli program to provide China with a counterpart of the US Airborne Warning and Control System (AWACS). Other forms of Russian defense-industrial assistance to China involving advanced submarines and tactical aircraft may also incorporate computation-intensive requirements that will be facilitated by Russia's ability to exploit the liberalization of export controls in the United States, Western Europe, and Japan. The liberalization of export controls which has benefited the Russian nuclear weapons complex appears to have had an even greater impact on China. China may have acquired more than fifty supercomputers since export controls were liberalized. Moreover, as China has rejected end-use controls by the United States, even on the few items still subject to a requirement for a validated export license, it is unlikely that the USG will be able monitor the potential diversion of supercomputers destined for "good" end users to defense/defense-industrial applications. Evidence that advanced technology industrial products from the US are routinely diverted from civil to military industrial uses emerged in the recent McDonnell Douglas machine tool case. In this circumstance, advanced machine tools intended for a civil application were diverted to the production of military aircraft.

It is likely that monitoring by the intelligence community of the end-use of uncontrolled high performance computers will be extensive. The decontrol of a significant fraction of high performance computer systems de facto diminishes their policy significance in terms pertinent to Executive branch resource allocation for monitoring and assessment. This circumstance produces another irony; the more extensive the pattern of export control liberalization of high performance computing, the less likely the USG is to be informed of the uses to which these systems are turned. Technological surprise in the national security field is inevitable in such circumstances and could be highly adverse to U.S. interests.

6.0 Overall implications of high performance computer exports for US national security interests.

High performance computing will be an integral element of scientific, industrial, and economic performance in the future for advanced economies. The commercial and technological success of high performance computing will inevitably be linked with the ability of US firms developing and producing high performance computing equipment to participate in the international market for these products.

High performance computing will be no less important for national security purposes. The recently completed Quadrennial Defense Review (QDR) has underscored the emphasis in defense modernization favoring computing-intensive military operations and support services as well as innovation in the U.S. defense-industrial base. The policy issue which must be addressed is to develop an approach which will harmonize the economic interest in developing an extensive international market for high performance computers while denying potential adversaries access to these powerful instruments of military performance.

An export control policy which fails to recognize and account for the implications of the dispersion of high performance computers to sensitive destinations and end-users invites technological surprise, regional instabilities, and renewed incentives on the part of nations threatened by weapons of mass destruction and their means of delivery, as well as advanced conventional weapons to undertake reciprocal initiatives. The search for offsetting capabilities in this manner is destabilizing, and inconsistent with long-term American national security interests. In this respect, export controls cannot be understood solely in terms of international commerce. They have a significant national security dimension as well.

The dynamism in the evolution of technology associated with high performance computation is a central factor affecting both the opportunities for the proliferation of WMD and advanced conventional weapons as well as the approach to the export control process. Computational modeling is becoming the "third leg" of science and engineering. The long-established "legs" of laboratory experiments and theoretical analysis have increasingly encountered limitations which computational modeling can address. The limitations of theoretical analysis are well-known: when problems are so complex that too many simplifying, but physically invalid, assumptions are needed, then analysis must give way to numerical computation and modeling. Although full-scale laboratory experiments are ideal, there are many times when they are too expensive, too dangerous, or from the perspective of potential proliferators – illegal (such as nuclear testing) to carry out. What is not brought out in the study with sufficient clarity is that numerical modeling and simulation used in conjunction with laboratory experiments that measure parts of, but not the entire problem (along with theoretical analysis) make a very potent tool. The Department of Energy's Science-Based Stockpile Stewardship program is based on this idea. Moreover, it can be argued, based on practical examples, that in the past five years, our skills in scientific computing (which must be distinguished from computer science) and large-scale modeling and simulation of complex systems have advanced even more rapidly than has computer hardware.

The dynamism of high performance computing technology poses significant demands on the regulatory process as well. The rate of change in the underlying technology requires continuous, not episodic regulatory reviews to separate commercial commodity-types of

computing hardware and software from advanced capabilities as a subject for export controls. The role of parallel processing to create teraflop or faster machines built from inexpensive computers may pose a future threat. The associated problem of parallel computing through Networks of Workstations (NOWs) poses particularly difficult problems for export control authorities. In due course, the problem may need to be addressed through controls on software and “peopleware” rather than sole dependence on hardware-based export controls.

The compilers, language extensions, etc., needed for NOWs are not readily available at the present time. In the future, it is likely to be practical to develop turn-key versions to be available via the Internet (including the compilers and languages, but also the libraries and high-level codes) that could complicate the export control process. However, parallel processing software requires intense supervision and maintenance to make it work effectively. Highly trained specialists in simulation and modeling with parallel processing machines – both computer scientists and computational modelers are needed. The role of technology transfer to nationals from proliferation-prone destinations through institutions of higher education in the United States and other advanced economies needs to be addressed in the context of the export control dimension of the problem of proliferation.

6.1 Foreign availability of high performance computers

In the 1980s when the export control regime for high performance computers was established, the US and Japan were the only producers of such systems. The limited and specialized market for high performance computing facilitated the management of the export control regime. The dispersion of advanced technology makes it likely that the number of sources for high performance computers will increase over time, creating the potential for foreign availability of these systems.

Provisions of existing law have recognized the issue of foreign availability for both dual-use and munitions list exports. In the case of dual-use exports, statutory provisions exist to prevent export denials for US firms where uncontrolled foreign availability exists. The issue is the degree to which nations abroad whose resident firms produce high performance computers can be drawn into an export control regime to limit the access of proliferation-prone end-users (e.g. Iran, Iraq, Libya, etc.) to these systems.

Diplomatic evidence suggests that it is feasible to do so. During the 1980s, the USG became concerned about the issue of the foreign availability of COCOM-controlled technology from non-COCOM member states. Twenty four nations were identified in this category. Diplomatic initiatives were undertaken by the US and a few other leading COCOM-member states which resulted in a parallel regime to enforce COCOM restrictions on the transfer of both COCOM-origin technology and locally produced/COCOM-controlled technology from being sent to COCOM-proscribed destinations.

The Clinton administration has successfully broadened the international constituency for non-proliferation through its advocacy. Moreover, subsequent events such as Iraq's various WMD programs, Iran's nuclear weapons program, and Libya's chemical weapons program have sensitized many nations to the risks associated with the proliferation of weapons of mass destruction and their means of delivery as well as advanced conventional weapons. As a consequence, a diplomatic initiative is likely to find a receptive audience in national capitals increasing the probability of success in managing the foreign availability issue.

Successful implementation of an international export control regime encompassing other nations producing high performance computing equipment will require effective intelligence support, law enforcement cooperation, and responsive diplomacy. Because of extensive export control liberalization, intelligence monitoring of the diversion of advanced dual use technologies to proliferation-prone end users has a low collection and processing priority in the intelligence community. Effective management of a regime involving foreign availability requires effective intelligence support for both the diplomatic and law enforcement dimensions of the problem. Equipped with timely intelligence support, diplomatic initiatives reinforced by effective collaboration between customs enforcement officials can significantly affect diversion channels usually exploited by proliferation-prone end users.

The control regime also requires clear regulatory thresholds to permit effective enforcement on an international basis. Doing so will place the regime within manageable bounds and permit an enforcement focus on the most significant dimension of the problem. The rapid changes in the technology as well as the market for computing equipment makes it necessary that the regulatory regime be responsive to the dynamism of the industry. Regulation needs to anticipate as well as adjust to contemporary technological change. This requirement is magnified if the USG seeks to manage an international regime to engage the foreign availability issue. Precedent suggests that the foreign availability of high performance computing technology to proliferation-prone end-users can be controlled if it becomes USG policy to do so.

6.2 Networking of uncontrolled computers to produce high performance systems

Networking of uncontrolled computers through dedicated hardware solutions in ways that produce a capability equal to or greater than controlled high performance computers may be practical in the future. This development makes it appropriate to manage such networking hardware and technical data for export licensing purposes parallel to the manner in which high performance computers are managed. Particular attention needs to be given to the construction of closed, "secret" or "classified" networks in proliferation concern countries.

In the future, it is plausible that networking of uncontrolled computers through software solutions implemented via internet links of multiple systems will be practical, even though significant obstacles remain before such an approach comes into widespread use. The architecture for such systems requires more study before regulatory conclusions can be drawn. However, from a regulatory perspective, there are analogs from USML licensing practice concerning the licensing of the transfer of technical data that may offer a practical regulatory solution. The policy aims are narrowly focused on a small number of proliferation-prone end-users making an export control regime for networked uncontrolled computers practical from a regulatory perspective.

It is important to keep in mind and distinguish between "secret" or "classified" networks and public networks. Countries involved in weapons proliferation will probably not desire to carry out their R&D across open networks. The Defense Department maintains a number of classified systems which are on closed, classified networks. There is growing evidence that China is building secret high performance networks to support supercomputers being obtained from the United States.

7.0 Recommendations

The US government has a continuing interest in the application of high performance computers for military purposes. The abandonment of export controls over most high performance computers since 1995 has produced a significant broadening of the distribution of such systems with diminished USG surveillance of the end users and the purposes for which the computers are used. A better understanding of the scope and consequences of the dissemination of high performance computers, and the ability of the Federal government to monitor and restrict the transfer of high performance computers and related capabilities to proliferation-sensitive destinations is needed.

7.1 Conduct an assessment of the military and defense-industrial significance of high performance computer exports to sensitive destinations

The Congress should request a timely (45 days) study by the Defense Intelligence Agency of the distribution of US and allied high performance computers to China, the former Soviet Union, Iran, Iraq, Syria, and Libya and to assess the impact of these transfers on:

- nuclear weapon design, development, manufacturing, performance and testing;
- chemical and biological weapon design, development, manufacturing, performance, and testing;
- the design, development, manufacture, performance, and testing of major weapon platforms including tactical aircraft, cruise/ballistic missiles, and submarines;

- antisubmarine warfare;
- command-control-communications
- intelligence collection, processing, and dissemination; and
- financial, commercial, government, and military communications, including encrypted communications.

The process of decontrol has materially degraded USG monitoring of foreign technology developments involving the use of uncontrolled “civil” sector technologies for military purposes. While many civil sector technologies are of limited importance for advanced military capabilities, this is not true of high performance computing.

7.2 Improve USG capabilities to monitor and restrict high performance computer transfers and associated services and technologies to sensitive destinations

Decontrol of high performance computer exports has diminished the ability of the USG to monitor, assess, and control the emergence of potential threats to the US and its allies facilitated by the access of adversary nations to high performance computers and associated technologies and services. Several measures should be considered to cope with these circumstances.

7.21 Replace export control regulations pertaining to the export of computers capable of performing more than 2,000 Mtops, and smaller systems capable of operations of more than 2,000 Mtops when linked or networked by dedicated hardware or software.

The existing supercomputer control regime is inadequate for national security purposes because sensitive end users have diverted these systems to threatening military applications. The existing regulations should be replaced by a licensing regime that would permit the USG to regain the ability to monitor, assess, and where necessary, control the distribution of high performance computing capabilities to sensitive destinations and end-users.

7.22 Require an individual validated export license for high performance computers with a capability of performing more than 500 Mtops and where the computers can be linked together and supported by hardware and/or soft enabling parallel processing, except for former COCOM member states, and other nations who agree not to re-export controlled computers, services, and associated hardware and software to sensitive destinations without prior USG

approval. Those nations who do so would be eligible to receive controlled items on the basis of a general license.

Instituting such a requirement would increase the ability of the USG, where appropriate, with allied nations, to restrain the flow of high performance computers to sensitive end users and destinations, without constraining the flow of such technology to legitimate end users throughout the world. It would also augment the recently negotiated Wassenaar Arrangement by strengthening the supercomputer control regime in parallel with international efforts to constrain the flow of advanced conventional weapons and technologies to sensitive destinations.

7.23 Broaden controls of network hardware and software associated with the linking or networking of high performance computers so that these elements are managed from a regulatory perspective parallel to high performance computers (or smaller machines, when linked or networked) are capable of achieving controlled levels of performance.

This measure establishes symmetric treatment for computer networking hardware and software in parallel with high performance computers that can be employed by sensitive end users in proliferation-prone destinations to create controlled high performance computing capabilities by networking smaller systems.

7.24 Hardware, software, and networking systems relating to computer security including firewalls, encryption, and network diagnostic technology related to computer security should be denied to sensitive end users and destinations.

Computer security and the networking of computers to create high performance computing systems in proliferation-prone destinations poses a risk to US security and the security of US regional allies placed in harms way by the development of weapons of mass destruction and their means of delivery as well as advanced conventional weapons. A licensing system supported by multilateral diplomacy was a practical means of preventing the militarily significant transfer of controlled technologies and equipment to the former Soviet bloc during the Cold War. The scale of this effort was considerably larger than is required to address controls over technologies associated with high performance computing.

7.25 High performance computing technology (hardware and software, components and systems) subject to export controls to sensitive destinations and end-users should be subject to continuous monitoring to make appropriate adjustments in export control criteria.

The dynamism of the technology underlying high performance computing is shifting the notion of what high performance computing is. Today's high performance computer is tomorrow's commodity-type of computer. Advances in high performance computing are creating new ways of facilitating proliferation which must be addressed by modern, effective, and appropriate approaches to export control.

Stephen Bryen
Former Director, Defense Technology
Security Administration, Department of Defense
(1981-88)

Professor Phil Marcus
College of Engineering
University of California, Berkeley

William R. Graham
Former Chairman of the U.S. General Advisory
Committee on Arms Control and Disarmament,
(1981-85) and Science Advisor to the President
(Dates)

William Schneider, Jr.
Former Under Secretary of State
for Security Assistance, Science
and Technology, US Department
of State (1982-86) and Chairman
of the U.S. General Advisory
Committee on Arms Control and
Disarmament (1987-93)

July 15, 1997

Professor Jack Dongarra
Computer Science Department
107 Ayres Hall
University of Tennessee
Knoxville, Tennessee 37996

July 28, 1997

The Honorable Floyd Spence
2405 Rayburn House Office Building
United States House of Representatives
Washington, DC 20515

The Honorable Ronald Dellums
2108 Rayburn House Office Building
United States House of Representatives
Washington, DC 20515

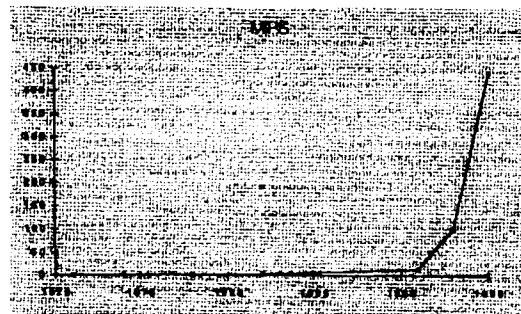
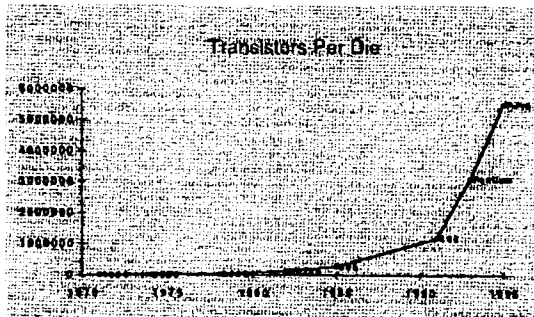
Dear Representatives Dellums and Spence,

First, I must apologize for not having time to review and respond to the full report on "An Assessment of the Impact of the Export of Advanced Computers and Computation Technology on the Proliferation of Conventional Weapons, Weapons of Mass Destruction, and Their Means of Delivery." I would like to limit my comments to the technical aspect of one of the report's recommendations. The report makes a number of statements that propose to set thresholds on export licensing based on absolute performance numbers. The performance number is in terms of millions of theoretical operations per second, or Mtops. I feel that whatever mechanism is used to monitor and regulate high-performance computer proliferation, must be both enforceable and have some validity over a long period. Both of these issues are very closely related. If the threshold for regulating high-performance computers is set at an unrealistically low level it will be difficult to adequately monitor the sales as such computers are currently almost at the commodity level. If the limit is static and based on some absolute quantity, these limits will be quickly surpassed given the rapid pace of technological advancement of microprocessor based system.

The current proposed limit for export control for Tier 3 countries is set at 7000 Mtops if the end-use and users are civilian; if the end-use and users are military the limit is set at 2000 Mtops for licensing. The current microprocessor based Personal Computer (PC) that can be purchased at the "corner store" is rated at 266 Mtops. This is the same computer you would consider purchasing for your home PC and such a purchase can take place at any electronics retail outlet store or phone mail-

order company. PC systems are available today that put together several of these commodity microprocessors within one "box". These machines are at the top of the line for household and office systems. Such top-of-the-line computers have two or even four processors in their systems. That puts commodity PC performance in the range of 1064 Mtops. Such systems are currently available from easily accessible sources. While in the San Francisco Bay area on a recent trip, I stopped at Fry's Electronics and priced such a system for \$3500. The ability to connect and "tie" such systems together into a parallel computer is also easily accomplished with software that is freely available on the Internet. For under \$10,000, one can easily assemble a system that will exceed the proposed limit.

The current trend in microprocessor growth is for the speed of the processor to double every 18 months. This effect was first noted or predicted by Gordon Moore (one of the founders of Intel) and goes by the name Moore's Law. This trend has been true for the last 10 years and is expected to hold true for the next 10 years. Gordon Moore's statement was actually about transistor density of semiconductor chips. The graphs below show the effect in terms of transistors per chip and the performance rate of the chips in terms of millions of instructions per second (MIPS), which is the equivalent of Mtops.



That puts the \$3500 commodity PC exceeding the threshold set for Tier 3 military use in a year and a half.

It would seem more realistic that a threshold be based on a formula that is indexed to the current commodity based microprocessor rather than an absolute number that quickly becomes out of date and presents unrealistic thresholds for regulations.

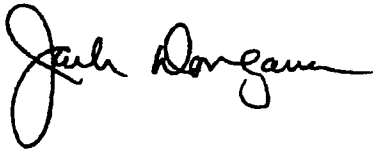
Perhaps the threshold set at say 100 times the current commodity microprocessor capability for Tier 2 countries would make sense. Anyone acquiring such a system is clearly interested in serious numerical computations. If we take the Intel Pentium II at 266 MHz as the commodity processor, then 100 times that rate puts the limit at 26,600 Mtops. The current proposed limit of 2,000 Mtops for military end-use sets

July 28, 1997

the limit at the equivalent of roughly 7 personal computers. I find it very hard to believe that such a limit can be effectively enforced.

Again, thank you for the opportunity to provide input to your committee.

Sincerely,
Jack Dongarra

A handwritten signature in black ink, appearing to read "Jack Dongarra". The signature is fluid and cursive, with the first name "Jack" and last name "Dongarra" clearly distinguishable.

Distinguished Professor
University of Tennessee
and
Distinguished Scientist
Oak Ridge National Laboratory